

**BURSOR & FISHER, P.A.**  
Joel D. Smith, Cal. Bar No. 244902  
Neal J. Deckant, Cal. Bar No. 322946  
1990 North California Blvd., Suite 940  
Walnut Creek, CA 94596  
Telephone: (925) 300-4455  
jsmith@bursor.com  
ndeckant@bursor.com

**GEORGE FELDMAN MCDONALD, PLLC**  
Lori G. Feldman (admitted *pro hac vice*)  
Michael Liskow, Cal. Bar No. 243899  
200 Park Avenue, Suite 1700  
New York, New York 10166  
Telephone: (646) 354-6534  
lfeldman@4-justice.com

**LOCKRIDGE GRINDAL NAUEN P.L.L.P.**  
Rebecca A. Peterson, Cal. Bar No. 241858  
Kate M. Baxter-Kauf (admitted *pro hac vice*)  
Robert K. Shelquist (*pro hac vice* forthcoming)  
100 Washington Avenue South, Suite 2200  
Minneapolis, MN 55401  
Telephone: (612) 339-6900  
rapeterson@locklaw.com  
kmbaxter-kauf@locklaw.com  
rkshelquist@locklaw.com

**THE HODA LAW FIRM, PLLC**  
Marshal J. Hoda (admitted *pro hac vice*)  
12333 Sowden Road, Suite B  
Houston, TX 77080  
Telephone: (832) 848-0036  
marshal@thehodalawfirm.com

**FOSTER YARBOROUGH PLLC**  
Patrick Yarborough (admitted *pro hac vice*)  
917 Franklin Street, Suite 220  
Houston, TX 77002  
Telephone: (713) 331-5254  
patrick@fosteryarborough.com

**EMERSON FIRM, PLLC**  
John G. Emerson (*pro hac vice* forthcoming)  
2500 Wilcrest Drive, Suite 300  
Houston, TX 77042-2754  
Telephone: (800) 551-8649  
jemerson@emersonfirm.com

*Attorneys for Plaintiffs*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

MARY L. SMITH, *et al.*, individually and on  
behalf of all others similarly situated,

Plaintiffs,

v.

GOOGLE, LLC.,

Defendant.

Case No. 5:23-cv-03527-PCP

**CONSOLIDATED CLASS ACTION  
COMPLAINT**

**JURY TRIAL DEMANDED**

1 **NATURE OF THE ACTION**

2 1. This is a putative class action against Defendant Google, LLC (“Google”) for  
3 wiretapping electronic communications on major on-line tax filing websites offered by H&R Block,  
4 TaxAct, and TaxSlayer, among others. As a result of this wiretapping, U.S. consumers have been  
5 involuntarily transmitting their sensitive financial information to Google when they file their taxes  
6 online. This information includes income, refund amounts, filing status, and scholarship  
7 information.

8 2. What made this wiretapping possible is Google Analytics’ tracking pixel, which is  
9 embedded in the JavaScript of online tax preparation websites. These tax preparation companies  
10 sent private tax return information to Google through Google Analytics and its embedded tracking  
11 pixel, which was installed on their websites.<sup>1</sup> These pixels sent massive amounts of user data to  
12 Google to improve its ad business and enhance its other business tools.<sup>2</sup>

13 3. Disclosing tax-return information without consent is a crime. *See* 26 U.S. § 7216.  
14 Aiding and abetting the unlawful disclosure of tax-return information is a crime. Inspecting  
15 unlawfully obtained tax-return information is a crime. *See* 26 U.S.C. § 7213A(a)(2).

16 4. This action is brought on behalf of Plaintiffs and a putative class of all people in the  
17 United States who used the online tax preparation providers such as H&R Block, TaxAct, or  
18 TaxSlayer, while those websites had the Google Analytics pixel installed on them. This action also  
19 seeks to certify putative subclasses of residents of various states who used the same websites. The  
20 complaint alleges violations of state and federal wiretapping laws.

21 **THE PARTIES**

22 5. Plaintiff Mary L. Smith is a citizen of DuPage County, Illinois. Since at least 2018,  
23 Plaintiff Smith has used H&R Block’s website to file her taxes online. At that time, the website  
24

25 \_\_\_\_\_  
26 <sup>1</sup> *See* United States Senate, *Attacks on Tax Privacy: How the Tax Prep Industry Enabled Meta to*  
27 *Harvest Millions of Taxpayers’ Sensitive Data* (July 2023), at 6, available at  
[https://www.warren.senate.gov/imo/media/doc/Attacks%20on%20Tax%20Privacy\\_Final.pdf](https://www.warren.senate.gov/imo/media/doc/Attacks%20on%20Tax%20Privacy_Final.pdf) (last  
28 accessed Sept. 24, 2023).

<sup>2</sup> *See id.*

1 utilized Google's tracking pixel.

2 6. Plaintiff Malissa Adams is a citizen of San Bernardino, California. Since at least  
3 2021, Plaintiff Adams has used TaxSlayer's website to file her taxes online. At that time, the website  
4 utilized Google's tracking pixel.

5 7. Plaintiff Tracylyn Patterson is a citizen of Brevard County, Florida. Since at least  
6 2020, Plaintiff Patterson has used TaxSlayer's website to file her taxes online. At that time, the  
7 website utilized Google's tracking pixel.

8 8. Plaintiff Cary Goldberg is a citizen of Broward County, Florida. Since at least 2014,  
9 Plaintiff Goldberg has used H&R Block's website to file his taxes online. At that time, the website  
10 utilized Google's tracking pixel.

11 9. Plaintiff Tyisha Sheppard is a citizen of Henry County, Georgia. Since at least 2015,  
12 Plaintiff Sheppard has used TaxSlayer's website to file her taxes online. At that time, the website  
13 utilized Google's tracking pixel.

14 10. Plaintiff Teresa Wright is a citizen of Sangamon County, Illinois. Since at least 2019,  
15 Plaintiff Wright has used TaxSlayer's website to file her taxes online. At that time, the website  
16 utilized Google's tracking pixel.

17 11. Plaintiff Rheazene Taylor is a citizen of Cook County, Illinois. Since at least 2018,  
18 Plaintiff Taylor has used TaxSlayer's website to file her taxes online. At that time, the website  
19 utilized Google's tracking pixel.

20 12. Plaintiff Tiffany Layton is a citizen of Westchester County, New York. Since at least  
21 2020, Plaintiff Layton has used TaxAct's website to file her taxes online. At that time, the website  
22 utilized Google's tracking pixel.

23 13. Plaintiff Jamila Armstrong is a citizen of Richland County, South Carolina. Since at  
24 least 2012, Plaintiff Armstrong has used either TaxAct's or TaxSlayer's websites to file her taxes  
25 online. At that time, the website utilized Google's tracking pixel.

26 14. Plaintiff Monica Townsend is a citizen of Harris County, Texas. Since at least 2021,  
27 Plaintiff Townsend has used TaxSlayer's website to file her taxes online. At that time, the website  
28 utilized Google's tracking pixel.



1 capabilities into its top revenue generating feature by including ads as results for Google searches.<sup>8</sup>  
2 Advertising on Google was launched in 2000 with the aim of connecting online businesses with users  
3 through “highly targeted ad serving technology” that enabled advertisers to monitor ad statistics such  
4 as click-through rates and visitor interest.<sup>9</sup> By 2016, Google earned nearly all of its revenue from  
5 advertising based on Google users’ search requests.<sup>10</sup>

6 20. In 2020, Google generated \$104 billion through advertising (71% of Google’s entire  
7 revenue for that year).<sup>11</sup> Google’s revenue from advertising is expected to reach \$201.05 billion by  
8 2024.<sup>12</sup>

9 21. Google offers several platforms and analytics for advertisers to optimize their  
10 advertising campaigns.<sup>13</sup> Advertisers using Google products can bid on specific search words and  
11 phrases that lead their ads to be more prominently displayed to relevant users in search results.<sup>14</sup>  
12 Google’s search advertising capabilities are so powerful that they enable advertisers to target a  
13 specific location, language and audience.<sup>15</sup> Google’s ads are not just embedded within Google search  
14 results, but also within other Google features such as Maps and YouTube.<sup>16</sup>

---

18 <sup>8</sup> *See id.*

19 <sup>9</sup> <https://www.blog.google/technology/ads/new-advertising-brands/> (last accessed Sept. 24, 2023);  
20 <http://googlepress.blogspot.com/2000/10/google-launches-self-service.html> (last accessed Sept. 24, 2023).

21 <sup>10</sup> *See* <https://www.britannica.com/topic/Google-Inc> (last accessed Sept. 24, 2023).

22 <sup>11</sup> *See* <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html> (last accessed Sept. 24, 2023).

23 <sup>12</sup> *See* <https://www.forbes.com/sites/bethkindig/2023/01/27/ad-budgets-set-to-slow-even-more-in-2023/?sh=6be6da1c554c> (last accessed Sept. 24, 2023).

24 <sup>13</sup> *See* <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html> (last accessed Sept. 24, 2023).

25 <sup>14</sup> *See id.*

26 <sup>15</sup> *See id.*

27 <sup>16</sup> *See* <https://www.business.com/articles/6-reasons-why-your-business-should-be-using-google-ads/> (last accessed Sept. 24, 2023).

22. Google prides itself on its “advanced” analytics products and services to provide advertisers a “holistic view into consumer behavior” to better target them.<sup>17</sup> To optimize advertising, Google offers data tracking features that track how users interact with ads and advertisers’ websites. For instance, Google will track and analyze what words or ads drove the most sales for any given Google customer and what days users clicked on search ads the most. Google is able to track groups of users “who have generated similar behavioral data or who share demographic or other descriptive data,” e.g., age group and gender.<sup>18</sup> In essence, Google’s mining of the data collected from users is what drives and makes so precise Google’s targeted advertising.

23. Google’s data collecting capabilities also include tracking user actions on customer websites and apps that are referred to as “events,” and important desired events (such as purchases) that are referred to as “conversions.”<sup>19</sup> Tracked conversions can be used to measure the effectiveness of ads and monitor user behavior.<sup>20</sup> Google also generates reports to give its advertising customers “post-click performance metrics for users who clicked on [a]ds and then came through [an advertiser’s] website, or installed and started using [an advertiser’s] mobile app.”<sup>21</sup> Google’s data collecting and reporting capabilities are encapsulated in its Google Analytics service.

### ***The Wiretapping Device: Google Analytics’ Tracking Pixel***

24. Google Analytics is a suite of business tools that Google claims help business and other website owners understand how visitors use their sites and apps.<sup>22</sup> It is a “platform that collects

---

<sup>17</sup> [https://blog.google/products/ads-commerce/5-tips-to-power-your-2023-marketing-strategy/?\\_ga=2.25524031.381675576.1689225706-1533121624.1689225706](https://blog.google/products/ads-commerce/5-tips-to-power-your-2023-marketing-strategy/?_ga=2.25524031.381675576.1689225706-1533121624.1689225706) (last accessed Sept. 24, 2023).

<sup>18</sup> <https://support.google.com/analytics/answer/12799087?hl=en&sjid=3548329945210241384-NA> (last accessed Sept. 24, 2023).

<sup>19</sup> <https://support.google.com/analytics/answer/13128484?sjid=11475162976737609263-NA> (last accessed Sept. 24, 2023).

<sup>20</sup> See <https://support.google.com/analytics/answer/13128484?sjid=11475162976737609263-NA> (last accessed Sept. 24, 2023); <https://support.google.com/analytics/answer/13366706?sjid=11475162976737609263-NA> (last accessed Sept. 24, 2023).

<sup>21</sup> [https://support.google.com/analytics/answer/4355493?hl=en&ref\\_topic=1308583&sjid=11475162976737609263-NA](https://support.google.com/analytics/answer/4355493?hl=en&ref_topic=1308583&sjid=11475162976737609263-NA) (last accessed Sept. 24, 2023).

<sup>22</sup> See *Some Facts About Google Analytics Data Privacy*, <https://blog.google/around-the-globe/google-europe/google-analytics-facts/> (last accessed Sept. 24, 2023).

1 data from [advertisers'] websites and apps to create reports that provide insights into [their]  
2 business.”<sup>23</sup> For example, Google Analytics helps website owners “understand which sections of an  
3 online newspaper have the most readers, or how often shopping cards are abandoned for an online  
4 store.”<sup>24</sup> Google Analytics allows its customers to collect such detailed information like the number  
5 of clicks, scrolls, searches, and downloads a site user performs.<sup>25</sup> The most recent version of Google  
6 Analytics offers a feature called Reporting Identity, which helps customers identify users by  
7 “creat[ing] a single user journey from all the data associated with the same identity.”<sup>26</sup> Google  
8 Analytics offers advertisers machine learning technology to uncover and predict new user insights  
9 such as their behavior and identifies new audiences of users likely to make a purchase.<sup>27</sup>

10 25. One such tool Google offers is Google Analytics’ embedded pixel, which is an  
11 invisible 1x1 web bug that website owners add to their website code for each page of their site to  
12 measure certain actions taken by users on the site, such as online purchases.<sup>28</sup> Of significance is that  
13 the tracking pixel is a default feature of Google Analytics.<sup>29</sup>

14 26. Google describes Google Analytics embedded pixel as follows: “Every time a user  
15 visits a webpage [with the code], the tracking code *will collect [purportedly] pseudonymous*  
16 *information about how that user interacted with the page.*”<sup>30</sup> The tracking pixel will also collect  
17 information from the browser like the language setting, the browser type, and the device and  
18 operating system on which the browser is running.<sup>31</sup> It can even collect the “traffic source,” which  
19 is what brought users to the site in the first place such as a search engine, an advertisement they

20 <sup>23</sup> <https://support.google.com/analytics/answer/12159447?hl=en> (last accessed Sept. 24, 2023).

21 <sup>24</sup> *Id.*

22 <sup>25</sup> See <https://www.mparticle.com/blog/google-tag-manager-vs-google-analytics/#:~:text=Google%20Analytics%20is%20an%20analytics,for%20granular%20user%20event%20insights> (last accessed Sept. 24, 2023).

23 <sup>26</sup> *Id.*

24 <sup>27</sup> See <https://blog.google/products/ads-commerce/prepare-for-future-with-google-analytics-4/> (last  
25 accessed Sept. 24, 2023).

26 <sup>28</sup> See <https://support.google.com/analytics/answer/12159447?hl=en> (last accessed Sept. 24, 2023).

27 <sup>29</sup> See *id.*

28 <sup>30</sup> *Id.*

<sup>31</sup> See *id.*

1 clicked on, or an email marketing campaign.<sup>32</sup> “When the tracking pixel collects data, it packages  
2 the information and sends it to Google Analytics to be processed into reports.”<sup>33</sup> The reports are  
3 then organized on particular criteria like whether a user’s device is mobile or desktop, or which  
4 browser they are using.<sup>34</sup> A Google Analytics customer can further configure the settings to allow  
5 them to customize what data is collected and how it is processed.<sup>35</sup>

6 27. The Google Analytics tracking pixel has vast capabilities and can collect a large range  
7 of user data of up to 200 different metrics, including the following according to Google:<sup>36</sup>

- 8 ☐ **Ad Interactions** – Includes when users are exposed to ads, when users click ads, and  
9 when ads grant rewards.
- 10 ☐ **Button Click Data** – Includes when users click links that lead outside of the current  
11 domain, when users click links leading to files, how often buttons are clicked, tracking  
12 common clicks, any buttons clicked by site visitors, when screen transitions occur,  
13 every time a user’s page loads or is changed by the active site, when a user scrolls to  
14 the bottom of a page, each time a user performs a site search, first time site visits, and  
15 when users use and submit forms.
- 16 ☐ **Enabling Options** – Google Analytics allows customers to enable “enhanced  
17 measurements” which allow for the collection of other types of optional data. The  
18 optional enhanced measurements do not require code changes; instead, once the  
19 options are enabled Google Analytics begins collecting the data. Examples of custom  
20 data events that can be collected include conversion events, page views based on  
21 browser history, scrolls, and site searches.

22 28. User website interactions and data collected by Google Analytics’ pixel are  
23 transmitted in real time to Google, where the information is stored and processed into reports. Once  
24 the data is processed and stored it cannot be changed.<sup>37</sup>

25 29. Google Analytics and the corresponding tracking pixel is not simply a “tool” utilized

---

26 <sup>32</sup> *Id.*

27 <sup>33</sup> *Id.*

28 <sup>34</sup> *See id.*

<sup>35</sup> *See id.*

<sup>36</sup> *See* [https://support.google.com/firebase/answer/9234069?sjid=13198096824834568666-NA&visit\\_id=638248819935482735-1615699485&rd=1](https://support.google.com/firebase/answer/9234069?sjid=13198096824834568666-NA&visit_id=638248819935482735-1615699485&rd=1) (last accessed Sept. 24, 2023); <https://support.google.com/analytics/answer/9216061?sjid=13198096824834568666-NA> (last accessed Sept. 24, 2023).

<sup>37</sup> *See* <https://support.google.com/analytics/answer/12159447?hl=en> (last accessed Sept. 24, 2023).



1 by website owners for their own purposes. Google offers these technologies to customers in a free  
2 version because Google benefits (and profits from) their use. Google can use the data it gleans from  
3 tools like the tracking pixel to power its algorithms, providing it insight into the habits of users across  
4 the internet. Indeed, the data obtained allows Google to amass huge amounts of data in a detailed  
5 dossier, or digital fingerprint, that it keeps on its users and other website visitors. To the benefit of  
6 Google, Google Analytics also includes a feature that allows it to integrate with other Google data  
7 collecting products such as Google Ads, Google Data Studio, Google AdSense, Google Optimize  
8 360, Google Ad Manager, and Google Search Console.<sup>38</sup>

9 30. Google Analytics is widely deployed across many industries.

10 31. Google Analytics has been available in some form to website developers since 2005.  
11 The most recent version of Google Analytics was adopted by Google on July 1, 2023.<sup>39</sup>

12 ***Google Secretly Hoovers Up Vast Amounts of Private Tax Return Information***

13 32. Enabled by Google's pixel and business tools, the tax filing services such as H&R  
14 Block, TaxAct, and TaxSlayer have been quietly transmitting sensitive financial information to  
15 Google when Americans file their taxes online.

16 33. The information sent to Google can be used by the company to power its advertising  
17 algorithms. As described above, the Google pixel is a snippet of code that is placed within the overall  
18 code of a website. If business uses Google Analytics, the pixel is placed by default.<sup>40</sup> Once placed  
19 on the website, the pixel downloads more code from Google, which then gathers valuable and  
20 sensitive information about website visitors and their activity. This information is then used by  
21 advertisers to understand their users' behaviors and shopping patterns, measure the performance of  
22 ad campaigns, and build an audience-base for future ad targeting. The data collected by Google is  
23 used by website publishers to better understand how people enter, use, and leave their websites.

24 34. Google features this pixel through its Google Analytics product. Google Analytics

25 <sup>38</sup> See [https://www.techtarget.com/searchbusinessanalytics/definition/Google-](https://www.techtarget.com/searchbusinessanalytics/definition/Google-Analytics#:~:text=Google%20Analytics%20includes%20features%20that,and%20integration%20with%20other%20applications)  
26 [Analytics#:~:text=Google%20Analytics%20includes%20features%20that,and%20integration%20](https://www.techtarget.com/searchbusinessanalytics/definition/Google-Analytics#:~:text=Google%20Analytics%20includes%20features%20that,and%20integration%20with%20other%20applications)  
with%20other%20applications (last accessed Sept. 24, 2023).

27 <sup>39</sup> See <https://support.google.com/analytics/answer/11583528?hl=en> (last accessed Sept. 24, 2023).

28 <sup>40</sup> See <https://support.google.com/analytics/answer/12159447?hl=en> (last accessed Sept. 24, 2023).

1 gives its partners the opportunity to “[u]nderstand how [their] customers interact across [their] sites  
2 and apps,” “anticipate future customer actions” with machine learning, and “optimize marketing  
3 performance.” Google Analytics can be implemented on certain websites without writing or copying  
4 any additional code at all, allowing for less technologically sophisticated businesses to utilize Google  
5 Analytics to collect certain information by default such as browser language, browser type, user  
6 clicks, user downloads, form interactions, and page titles. Also by default, Google Analytics matches  
7 that information with users’ geolocation, gender, and general interests. This information is then  
8 provided to the customer in an aggregated form, accessible through the customer’s Google Analytics  
9 account dashboard.

10 35. For more sophisticated businesses, Google gives the option to install a pixel, called  
11 the Google Tag, directly on individual web pages. This allows website publishers to customize the  
12 type of data they want collected by Google.<sup>41</sup>

13 36. H&R Block, TaxAct, and TaxSlayer are some of the most widely used e-filing  
14 services that had the tracking pixel deployed on their websites.

15 37. The type of data collected by these sites may include email addresses, data on users’  
16 income, filing status, refund amounts, buttons that were clicked, and year of return.

17 38. H&R Block, which also has millions of users, reportedly transmitted information  
18 about tax filers’ filings to Google, and Google has admitted that its technology would permit such  
19 transmissions. Each Plaintiff was one of those users when he or she filed their taxes in the years  
20 2019 to the present. Since the tracking pixel was on the site at that time, and it operates always and  
21 for everyone, Plaintiffs’ tax return data would have been sent to Google. In a recently published  
22 Senate investigation, TaxAct revealed that the dollar amount of adjusted gross income and refund  
23 amounts were disclosed to Google.<sup>42</sup>

24 39. TaxSlayer reportedly used the Google Analytics tracking pixel embedded on the  
25 company’s website since March 2011. TaxSlayer completed 10 million federal and state tax returns

26 <sup>41</sup> See <https://support.google.com/analytics/answer/12131703?sjid=5199951762458264308-NA>  
27 (last accessed Sept. 24, 2023).

28 <sup>42</sup> United States Senate, *Attacks on Tax Privacy: How the Tax Prep Industry Enabled Meta to Harvest Millions of Taxpayers’ Sensitive Data*, at 6.

1 last year. In a recently published Senate investigation, TaxSlayer revealed that dollar amount of  
2 adjusted gross income and refund amounts were disclosed to Google.<sup>43</sup>

3 40. Google would have known, or at best recklessly turned a blind eye to, the fact that it  
4 was collecting vast amounts of confidential tax information. Income and other related financial  
5 information are highly valuable demographic markers for advertising purposes.

6 41. Concerning the anonymity of the sensitive information collected, Google claims such  
7 information is not associated with the user's name or other identifiable information making it so that  
8 the information is not able to be linked to a specific user. However, a Stanford and Princeton study  
9 found that Google's tracking software is able to "successfully carry out de-anonymization" through  
10 a simple process that leverages a user's web browsing history collected by Google's tracking tools.<sup>44</sup>  
11 Regardless, data can be compiled and used by Google Analytics customers to target ad content,  
12 limiting the extent that anonymity can be protected. Further, Google company officials have  
13 admitted that if a Google Analytics customer so desired, they would be able to configure their settings  
14 to track sensitive taxpayer information such as adjusted gross income, and Google's systems would  
15 not filter this information or even alert anyone.

16 42. Google purports to have policies in place that prohibit its Google Analytics customers  
17 from "passing any information that could be used by Google to identify individuals." Google further  
18 claims that "[c]ustomers who violate [their] policies are subject to account suspension or  
19 termination."<sup>45</sup> Yet Google has admitted to never having contacted any of the tax preparation  
20 companies about their sharing potentially sensitive information with Google, and it did not suspend  
21 or terminate any of the tax prep company accounts at any time.

22 43. Evidence obtained as part of the recent Senate investigation appears to indicate that  
23 Google "failed to implement adequate safeguards to prevent the transfer of taxpayers' sensitive  
24 personal and financial information, despite their contentions that they did so."<sup>46</sup>

---

25 <sup>43</sup> See *id.* at 37.

26 <sup>44</sup> See *id.* at 15.

27 <sup>45</sup> See *id.* at 20.

28 <sup>46</sup> See *id.* at 18.

1  
2 ***Google Did Not Receive Consent To Receive Confidential Tax Information***

3 44. The Internal Revenue Code states that a tax return preparer may not disclose “any  
4 information furnished to him for, or in connection with, the preparation of any such return” or use  
5 “any such information for any purpose other than to prepare, or assist in preparing any such return.”  
6 26 U.S.C. § 7216 (a). Thus, taxpayers can (and do) furnish their returns and return information, *i.e.*,  
7 income, refund amount, and filing status, to tax prep companies presumably with confidence that  
8 their privacy will be maintained. Tax return information protected by law includes information that  
9 the taxpayer provided solely for tax preparation purposes. Under the Code, this information is  
10 prohibited from disclosure unless the taxpayer gives permission to do so. *See id.* Further,  
11 “disclosure” is defined as “the act of making tax return information known to any person in any  
12 manner whatever.” 26 C.F.R. 301.7216-1(b)(5).

13 45. Google Analytics ultimately provides tax prep companies with statistical  
14 compilations of data, but the information these compilations are based on was apparently not in a  
15 compiled form until Google received and compiled it. Further, the data shared with Google was not  
16 truly anonymous regarding taxpayer identity because the information could, at the very least, be  
17 indirectly associated with a particular taxpayer.

18 46. Google also makes false representations and/or warranties that it does not collect  
19 sensitive information like the information at issue here.

20 47. For Google customers who connect their Google Analytics account to Google’s  
21 advertising products, the Google Analytics Advertising Features Policies apply. Google’s  
22 Advertising Policies expressly provide that website developers will not share data that includes  
23 health, ***financial*** or other categories of sensitive information. However, Google does not enforce  
24 this policy.

25 **CLASS ACTION ALLEGATIONS**

26 48. Plaintiffs seek to represent the following classes and subclasses:

27 Nationwide Class (or “class”): All people in the United States who used online tax  
28 preparation providers such as H&R Block, TaxAct, or TaxSlayer, while those  
websites had the Google pixel installed on them.

1        California Subclass: All people in California who used online tax preparation  
2 providers such as H&R Block, TaxAct, or TaxSlayer, while those websites had the  
Google pixel installed on them.

3        Florida Subclass: All people in Florida who used online tax preparation providers  
4 such as H&R Block, TaxAct, or TaxSlayer, while those websites had the Google  
pixel installed on them.

5        Illinois Subclass: All people in Illinois who used online tax preparation providers  
6 such as H&R Block, TaxAct, or TaxSlayer, while those websites had the Google  
pixel installed on them.

7        Texas Subclass: All people in Texas who used online tax preparation providers  
8 such as H&R Block, TaxAct, or TaxSlayer, while those websites had the Google  
pixel installed on them.

9            49.        Plaintiffs reserve the right to modify the class definition, including by using additional  
10 subclasses, as appropriate based on further investigation and discovery obtained in the case.

11           50.        Members of the putative class and subclasses are so numerous that their individual  
12 joinder herein is impracticable. On information and belief, members of the putative class and  
13 subclasses number in the millions. The precise number of putative class and subclass members and  
14 their identities are unknown at this time but may be determined through discovery. Putative class  
15 and subclass members may be notified of the pendency of this action by mail and/or publication  
16 through the distribution records of Google.

17           51.        Common questions of law and fact exist as to all putative class and subclass members  
18 and predominate over questions affecting only individual class members. Common legal and factual  
19 questions include, but are not limited to, whether Defendant has violated wiretapping statutes at issue  
20 here; and whether class members are entitled to statutory damages for the violations.

21           52.        The claims of the named Plaintiffs are typical of the claims of the putative class and  
22 subclasses because the named Plaintiffs, like all other class members, visited the websites of H&R  
23 Block, TaxAct, or TaxSlayer and had their electronic communications intercepted and disclosed to  
24 Google using the tracking pixel and/or other business tools.

25           53.        Plaintiffs are adequate representatives of the putative class and subclasses because  
26 their interests do not conflict with the interests of the class members they seek to represent, because  
27 they have retained competent counsel experienced in prosecuting class actions, and they intend to  
28

1 prosecute this action vigorously. The interests of putative class and subclass members will be fairly  
2 and adequately protected by Plaintiffs and their counsel.

3 54. The class mechanism is superior to other available means for the fair and efficient  
4 adjudication of the claims of putative class and subclass members. Each individual putative class  
5 and subclass member may lack the resources to undergo the burden and expense of individual  
6 prosecution of the complex and extensive litigation necessary to establish Defendant's liability.  
7 Individualized litigation increases the delay and expense to all parties and multiplies the burden on  
8 the judicial system presented by the complex legal and factual issues of this case. Individualized  
9 litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class  
10 action device presents far fewer management difficulties and provides the benefits of single  
11 adjudication, economy of scale, and comprehensive supervision by a single court on the issue of  
12 Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants  
13 are before this Court for consistent adjudication of the liability issues.

14 55. Plaintiffs bring all claims in this action individually and on behalf of members of the  
15 putative class and subclasses against Defendant.

16 **COUNT I**  
17 **Violation of the California Invasion of Privacy Act ("CIPA"),**  
18 **California Penal Code § 631**

19 56. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set  
20 forth herein.

21 57. Plaintiffs bring this claim individually and on behalf of the members of the putative  
22 class and subclasses against Defendant.

23 58. To establish liability under Section 631(a) of CIPA, a plaintiff need only establish  
24 that the defendant, "by means of any machine, instrument, contrivance, or in any other manner,"  
25 does any of the following:

26 Intentionally taps, or makes any unauthorized connection, whether  
27 physically, electrically, acoustically, inductively or otherwise, with  
28 any telegraph or telephone wire, line, cable, or instrument, including  
the wire, line, cable, or instrument of any internal telephonic  
communication system,

Or

1 Willfully and without the consent of all parties to the communication,  
2 or in any unauthorized manner, reads or attempts to read or learn the  
3 contents or meaning of any message, report, or communication while  
the same is in transit or passing over any wire, line or cable or is being  
sent from or received at any place within this state,

4 Or

5 Uses, or attempts to use, in any manner, or for any purpose, or to  
6 communicate in any way, any information so obtained,

7 Or

8 Aids, agrees with, employs, or conspires with any person or persons  
9 to unlawfully do, or permit, or cause to be done any of the acts or  
things mentioned above in this section.

10 59. Section 631(a) of CIPA is not limited to phone lines, but also applies to “new  
11 technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, Case No. 15-  
12 CV-04062-LHK, 2016 WL 8200619, at \*21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new  
13 technologies” and must be construed broadly to effectuate its remedial purpose of protecting  
14 privacy); *Bradley v. Google, Inc.*, No. C 06-05289 WHA, 2006 WL 3798134, at \*5-6 (N.D. Cal.  
15 Dec. 22, 2006) (CIPA governs “electronic communications”); *In re Facebook, Inc. Internet Tracking*  
16 *Litigation*, 956 F.3d 589 (9th Cir. Apr. 9, 2020) (reversing dismissal of CIPA and common law  
17 privacy claims based on Facebook’s collection of consumers’ Internet browsing history).

18 60. The tracking pixel and related business tools are a “machine, instrument, contrivance,  
19 or ... other manner” used to engage in the prohibited conduct at issue here.

20 61. At all relevant times, by using the Google Analytics Pixel, Defendant intentionally  
21 tapped, electrically or otherwise, the lines of internet communication between Plaintiffs and class  
22 members and the owners of the websites at issue here.

23 62. At all relevant times, by using the Google Analytics Pixel, Defendant willfully and  
24 without the consent of all parties to the communication, or in any unauthorized manner, read or  
25 attempted to read or learn the contents or meaning of electronic communications of Plaintiffs and  
26 putative class members, while the electronic communications were in transit or passing over any  
27 wire, line or cable or were being sent from or received at any place within California.

28 63. Plaintiffs and putative class and subclass members did not consent to any of

1 Defendant's actions in implementing the wiretaps. Plaintiffs and putative class and subclass  
2 members did not consent to Google's access, interception, reading, learning, recording, and  
3 collection of Plaintiffs' and putative class and subclass members' electronic communications.

4 64. Plaintiffs and putative class and subclass members seek all relief available under Cal.  
5 Penal Code § 637.2, including injunctive relief and statutory damages of \$5,000 per violation.

6 **COUNT II**  
7 **Violation of the California Invasion of Privacy Act ("CIPA"),**  
8 **California Penal Code § 632**

9 65. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth  
10 herein.

11 66. Plaintiffs bring this Count individually and on behalf of the members of the putative  
12 class and subclasses against Defendant.

13 67. The California Invasion of Privacy Act ("CIPA") is codified at Sections 630 to 638  
14 of the California Penal code. The Act begins with its statement of purpose:

15 The Legislature hereby declares that advances in science and technology have led to  
16 the development of new devices and techniques for the purpose of eavesdropping  
17 upon private communications and that the invasion of privacy resulting from the  
18 continual and increasing use of such devices and techniques has created a serious  
19 threat to the free exercise of personal liberties and cannot be tolerated in a free and  
20 civilized society.

21 CAL. PENAL CODE § 630.

22 68. Section 632(a) provides, in pertinent part:

23 A person who, intentionally and without the consent of all parties to a confidential  
24 communication, uses an electronic amplifying or recording device to eavesdrop upon  
25 or record the confidential communication, whether the communication is carried on  
26 among the parties in the presence of one another or by means of a telegraph,  
27 telephone, or other device, except a radio, shall be punished by a fine not exceeding  
28 two thousand five hundred dollars (\$2,500) per violation.

69. A defendant must show it had the consent of all parties to a communication.

70. Google's pixel and related backend and frontend code is "an electronic amplifying or  
recording device" under CIPA.

71. The data collected by Google constitutes "confidential communications," as that term  
is used in Section 632 of CIPA, because class members had objectively reasonable expectations of  
privacy with respect to their tax filing information.



72. Pursuant to Section 637.2 of the California Penal Code, Plaintiffs and putative class and subclass members have been injured by the violations of Section 635, and each seek damages for the greater of \$5,000 or three times the amount of actual damages, as well as injunctive relief.

**COUNT III**  
**Violation of the California Invasion of Privacy Act (CIPA),**  
**California Penal Code § 635**

73. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

74. Plaintiffs bring this claim individually and on behalf of the members of the putative class and subclasses against Defendant.

75. Section 635 of the California Penal Code provides, in pertinent part:

Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones or between a cellular radio telephone and a landline telephone in violation of Section 632.5, or communications between cordless telephones or between a cordless telephone and a landline telephone in violation of Section 632.6, shall be punished by a fine not exceeding two thousand five hundred dollars

....

76. At all relevant times, by implementing Google's wiretaps, Google intentionally manufactured, assembled, sold, offered for sale, advertised for sale, possessed, transported, imported, and/or furnished a wiretap device that is primarily or exclusively designed or intended for eavesdropping upon the communication of another.

77. The Google Analytics Pixel is a “device” that is “primarily or exclusively designed” for eavesdropping. That is, the Google Analytics Pixel is designed to gather information about what URLs users visit and what they search for.

78. Plaintiffs and putative class and subclass members did not consent to any of Defendant's actions in implementing Google's wiretaps.

79. Pursuant to Section 637.2 of the California Penal Code, Plaintiffs and putative class and subclass members have been injured by the violations of Section 635 of the California Penal

Code, and each seek damages for the greater of \$5,000 or three times the amount of actual damages, as well as injunctive relief.

**COUNT IV**  
**Violation of the Federal Wiretap Act,**  
**18 U.S.C. §§ 2510, *et seq.***

80. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

81. Plaintiffs bring this claim individually and on behalf of the members of the putative class and subclasses against Defendant.

82. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communications through the use of a device. *See* 18 U.S.C. § 2511.

83. The Federal Wiretap Act protects both the sending and receiving of communications.

84. Section 2520(a) of the Federal Wiretap Act provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

85. Google's actions in intercepting and tracking the information at issue here were intentional and done for the purpose of violating laws prohibiting the unlawful disclosure and review of tax information.

86. Google's intentional interception of internet communications that Plaintiffs and Class members were sending and receiving while navigating websites that integrated Google Analytics was done contemporaneously with the Plaintiffs' and Class members' sending and receipt of those communications.

87. The communications intercepted by Google included "contents" of electronic communications made by Plaintiffs.

88. The transmission of data between the tax-filing service websites and Class members were "transfer[s] of signs, signals, writing, ... data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetics, photoelectronic, or photooptical system that

affects interstate commerce[.]” and were therefore “electronic communications” within the meaning of Section 2510(12) of the Federal Wiretap Act. *See* 18 U.S.C. § 2510(12).

89. Google’s pixel and business tools are “devices” within the meaning of Section 2510(5) of the Wiretap Act. *See* 18 U.S.C. § 2510(5).

90. Google was not an authorized party to the communications because Plaintiffs and Class members were unaware of Google’s monitoring. Class members did not consent to Google’s interception or continued gathering of the user’s communications.

91. The interceptions by Google were unlawful and tortious, and were done in furtherance of one or more crimes baring disclosure or review of confidential tax information, and tortious invasion of privacy.

92. After intercepting the communications, Google used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of Section 2511(a) of the Federal Wiretap Act. 18 U.S.C. § 2511(a).

93. Plaintiffs and putative class and subclass members seek all available relief for the violations asserted here.

**COUNT V**  
**Violation of the Federal Wiretap Act,**  
**18 U.S.C. § 2512**

94. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

95. Plaintiffs bring this claim individually and on behalf of the members of the putative class and subclasses against Defendant.

96. Section 2512 of the Federal Wiretap Act, in pertinent part, holds “any person” liable who manufactures, assembles, or sells “any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. *See* 18 U.S.C. § 2512(1)(b).

97. The technology at issue here is an “electronic, mechanical, or other device” as defined by Section 2510(5) of the Federal Wiretap Act and is primarily useful for the purpose of the surreptitious interception of electronic communications. *See* 18 U.S.C. § 2510(5).

98. Defendant manufactured, marketed, and sold its technology with knowledge that it would primarily be used to illegally intercept electronic communications.

99. Defendant's conduct violated Section 2512 of the Federal Wiretap Act and therefore gives rise to a claim under Section 2520 of the Federal Wiretap Act. 18 U.S.C. §§ 2512, 2520.

100. Pursuant to Section 2520, Plaintiffs and the putative class and subclass are entitled to the greater of actual damages or statutory damages or not less than \$100 a day for each day of violation or \$10,000, whichever is greater. 18 U.S.C. § 2520.

**COUNT VI**  
**Violation of the Florida Security of Communications Act,**  
**Florida Statutes § 934.10**

101. Plaintiffs Patterson and Goldberg repeat the allegations contained in the paragraphs above as if fully set forth herein.

102. Plaintiffs Patterson and Goldberg bring this claim individually and on behalf of the members of the Florida Subclass against Defendant.

103. Florida’s Security of Communications Act, Fla. Stat. § 934.03, *et seq.*, provides that any person whose wire, oral, or electronic communication is intentionally intercepted, disclosed, or used in violation of the statute may bring a civil cause of action against any person or entity who “intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications.”

104. The Florida Security of Communications Act prohibits companies from intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept any wire, oral, or electronic communication without the prior consent of all parties to the communication.

105. Google's conduct violated the Florida Security of Communications Act because Google intentionally intercepted and/or recorded, by device or otherwise, private communications

1 between Plaintiffs Patterson and Goldberg and Florida Subclass members and their online tax-filing  
2 service providers, as described more fully herein, without first obtaining Plaintiffs Patterson and  
3 Goldberg and Florida Subclass members' consent.

4 106. Plaintiffs Patterson and Goldberg and the Florida Subclass members suffered harm as  
5 a result of Google's violations of the Florida Security of Communications Act, and therefore seek all  
6 available relief under that statute.

7 **COUNT VII**  
8 **Violation of the Illinois Eavesdropping Act,**  
9 **720 ILCS 5/14-6**

10 107. Plaintiffs Wright and Taylor repeat the allegations contained in the paragraphs above  
11 as if fully set forth herein.

12 108. Plaintiffs Wright and Taylor bring this claim individually and on behalf of the  
13 members of the Illinois Subclasses against Defendant.

14 109. The Illinois Eavesdropping Act, 720 ILCS 5/14-1, *et seq.*, provides that a person or  
15 entity commits eavesdropping when said person or entity knowingly and intentionally "[i]ntercepts,  
16 records, or transcribes, in a surreptitious manner, any private electronic communication to which he  
17 or she is not a party unless he or she does so with the consent of all parties to the private electronic  
18 communication." The Act further establishes under any person aggrieved by a violation of its  
19 provisions has a civil cause of action against violators. *See* 720 ILCS 5/14-6.

20 110. Google's conduct violated the Illinois Eavesdropping Act because Google  
21 intentionally intercepted and/or recorded, by device or otherwise, private communications between  
22 Plaintiffs Wright and Taylor and Illinois Subclass members and their online tax-filing service  
23 providers, as described more fully herein, without first obtaining class members' consent.

24 111. Plaintiffs Wright and Taylor and the Illinois Subclass members suffered harm as a  
25 result of Google's violations of the Eavesdropping Act, and therefore seek all available relief under  
26 that statute.

1 **COUNT VIII**

2 **Violation of the Texas Criminal Wiretap Act (Texas Code of Criminal Procedure, Article**  
3 **18A.502(1); and Texas Penal Code Sections 16.02(b)(1)–(b)(3), (b)(5))**

4 112. Plaintiff Townsend repeats the allegations contained in the paragraphs above as if  
5 fully set forth herein.

6 113. Plaintiff Townsend brings this claim individually and on behalf of the members of  
7 the Texas Subclasses against Defendant.

8 114. Section 16.02(b) of the Texas Penal Code criminalizes the intentional interception,  
9 disclosure, or use of electronic communications, and Article 18A.502 of the Texas Code of Criminal  
10 Procedure provides that a victim may bring a civil cause of action against a person or entity who  
11 commits such offenses against him or her. These two statutes are collectively known as the “Texas  
12 Criminal Wiretap Act.” Under the Texas Criminal Wiretap Act, it is a crime for companies to  
13 intercept private electronic communications without the consent of all parties to the communication  
14 where the communication is intercepted for the purpose of committing an unlawful act. *See* TEX.  
15 PEN. CODE § 16.02(c)(4)(B).

16 115. Google’s conduct violated Section 16.02(b) of the Texas Penal Code because Google  
17 intentionally intercepted electronic communications, private communications between Plaintiff  
18 Townsend and the Texas Subclass members and their online tax-filing service providers, as described  
19 more fully herein, without first obtaining class members’ consent.

20 116. Google intercepted Plaintiff Townsend and the Texas Subclass members’ tax-return  
21 information so that it could use that information in the consumer-information databases that it sells  
22 to advertisers. The unauthorized receipt and use of tax-return information is an unlawful act. *See*  
23 26 U.S.C. § 7213. Accordingly, Google intercepted Plaintiff Townsend and the Texas Subclass  
24 members’ communications with their tax-filing services for the purpose of committing an unlawful  
25 act and is thus liable under the statute.

26 117. Plaintiff Townsend and the Texas Subclass members suffered harm as a result of  
27 Google’s violations of the Texas Criminal Wiretap Act, and therefore seek all available relief under  
28 that statute.

1 **PRAYER FOR RELIEF**

2 WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek  
3 judgment against Google, as follows:

- 4 a. For an order certifying the putative class and subclasses and naming Plaintiffs as the  
5 representatives of the putative class and subclasses and Plaintiffs' attorneys as Class  
6 Counsel to represent the putative class and subclass members;
- 7 b. For an order declaring that the Defendant's conduct violates the statutes referenced  
8 herein;
- 9 c. For an order finding in favor of Plaintiffs and the putative class and subclasses on all  
10 counts asserted herein;
- 11 d. For statutory damages in amounts to be determined by the Court and/or jury;
- 12 e. For prejudgment interest on all amounts awarded;
- 13 f. For injunctive relief as pleaded or as the Court may deem proper; and
- 14 g. For an order awarding Plaintiffs and the putative class and subclass their reasonable  
15 attorneys' fees and expenses and costs of suit.

16 **JURY TRIAL DEMANDED**

17 Plaintiffs demand a trial by jury on all claims so triable.  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 Dated: October 9, 2023

Respectfully submitted,

2 **BURSOR & FISHER, P.A.**

3 By: /s/ Joel D. Smith

4 Joel D. Smith, Cal. Bar No. 244902  
5 Neal J. Deckant, Cal. Bar No. 322946  
6 1990 North California Blvd., Suite 940  
7 Walnut Creek, CA 94596  
8 Telephone: (925) 300-4455  
9 Facsimile: (925) 407-2700  
10 E-mail: jsmith@bursor.com  
11 Email: ndeckant@bursor.com

12 **GEORGE FELDMAN MCDONALD, PLLC**

13 Lori G. Feldman, *Admitted Pro Hac Vice*  
14 Michael Liskow, Cal. Bar No. 243899  
15 200 Park Avenue, Suite 1700  
16 New York, New York 10166  
17 Telephone: (646) 354-6534  
18 Email: lfeldman@4-justice.com  
19 Email: mliskow@4-justice.com

20 **LOCKRIDGE GRINDAL NAUEN P.L.L.P.**

21 Rebecca A. Peterson, Cal. Bar No. 241858  
22 Robert K. Shelquist, *Pro Hac Vice Forthcoming*  
23 Kate M. Baxter-Kauf, *Admitted Pro Hac Vice*  
24 100 Washington Avenue South, Suite 2200  
25 Minneapolis, MN 55401  
26 Telephone: (612) 339-6900  
27 Facsimile: (612) 339-0981  
28 E-mail: rapeterson@locklaw.com  
Email: rkshelquist@locklaw.com  
Email: kmbaxter-kauf@locklaw.com

**THE HODA LAW FIRM, PLLC**

Marshal J. Hoda, *Admitted Pro Hac Vice*  
12333 Sowden Road, Suite B, PMB 51811  
Houston, TX 77080  
Telephone: (832) 848-0036  
E-mail: marshal@thehodalawfirm.com

**FOSTER YARBOROUGH PLLC**

Patrick Yarborough, *Admitted Pro Hac Vice*  
917 Franklin Street, Suite 220  
Houston, TX 77002  
Telephone: (713) 331-5254  
Facsimile: (713) 513-5202  
Email: patrick@fosteryarborough.com



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**EMERSON FIRM, PLLC**

John G. Emerson, *Pro Hac Vice Forthcoming*  
2500 Wilcrest Drive, Suite 300  
Houston, TX 77042-2754  
Telephone: (800) 551-8649  
Facsimile: (501) 286-4659  
Email: jemerson@emersonfirm.com

*Attorneys for Plaintiff*